1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI

010813429 **Image available**
WPI Acc No: 96-310382/199632
XRPX Acc No: N96-260818

Processor-controlled exchange of cryptographic keys, e.g. in mobile communications - exchanging keys between network computer and user computer using Diffie-Hellman key exchange principle, and testing responses at both computers

Patent Assignee: SIEMENS AG (SIEI)
Inventor: HORN G; KESSLER V; MUELLER K

Number of Countries: 024 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
DE 19514084	C1	19960711	DE 1014084	A	19950413	H04L-009/00	199632 B
KR 98703838	A	19981205	WO 96DE591	A	19960403	H04L-009/08	200006
			KR 97707238	A	19971013		
WO 9632791	A1	19961017	WO 96DE591	A	19960403	H04L-009/08	199647
EP 820670	A1	19980128	EP 96908004	A	19960403	H04L-009/08	199809
			WO 96DE591	A	19960403		
JP 10510692	W	19981013	JP 96530635	A	19960403	H04L-009/08	199851
			WO 96DE591	A	19960403		

Priority Applications (No Type Date): DE 1014084 A 19950413
Cited Patents: Jnl.Ref; EP 393806
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
DE 19514084	C1		10			
KR 98703838	A			Based on		WO 9632791
WO 9632791	A1	G	27			
Designated States (National): CN JP KR RU UA US						
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE						
EP 820670	A1	G		Based on		WO 9632791
Designated States (Regional): AT CH DE ES FR GB IT LI						
JP 10510692	W		26	Based on		WO 9632791

Abstract (Basic): DE 19514084 C

Cryptographic keys are exchanged by generating a first coincidence number on the network computer (N). A first message is transmitted from a network computer to a subscriber computer which generates a second coincidence number. The second coincidence number generates a value which enables an open network key. The subscriber computer calculates an encrypted term (VT1). The subscriber computer generates a second message which contains at least the value generated by the second coincidence number, the first encrypted term, and the first response (A).

The second message is transmitted from the subscriber computer to the network computer. The first response is tested in the network computer. The network computer then sends a third message which includes at least a second response (B) which is tested in the subscriber computer.

USE/ADVANTAGE - Confidential information system. Explicit authentication of code messages by network computer and subscriber computer.

Dwg.1a/2

Title Terms: PROCESSOR; CONTROL; EXCHANGE; CRYPTOGRAPHIC; KEY; MOBILE; COMMUNICATE; EXCHANGE; KEY; NETWORK; COMPUTER; USER; COMPUTER; KEY; EXCHANGE; PRINCIPLE; TEST; RESPOND; COMPUTER
Derwent Class: P85; T01; W01
International Patent Class (Main): H04L-009/00; H04L-009/08
International Patent Class (Additional): G06F-012/14; G09C-001/00; H04L-009/32

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平10－510692

(43)公表日　平成10年(1998)10月13日

(51)Int.Cl.[6]		識別記号	Ｆ Ｉ		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｄ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６０１Ｅ
					６７５Ｂ

審査請求　有　　予備審査請求　有　（全 26 頁）

(21)出願番号　特願平8－530635
(86)(22)出願日　平成８年(1996)４月３日
(85)翻訳文提出日　平成９年(1997)10月13日
(86)国際出願番号　ＰＣＴ／ＤＥ９６／００５９１
(87)国際公開番号　ＷＯ９６／３２７９１
(87)国際公開日　平成８年(1996)10月17日
(31)優先権主張番号　１９５　１４　０８４．２
(32)優先日　1995年４月13日
(33)優先権主張国　ドイツ（ＤＥ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＮ，ＪＰ，ＫＲ，ＲＵ，ＵＡ，ＵＳ

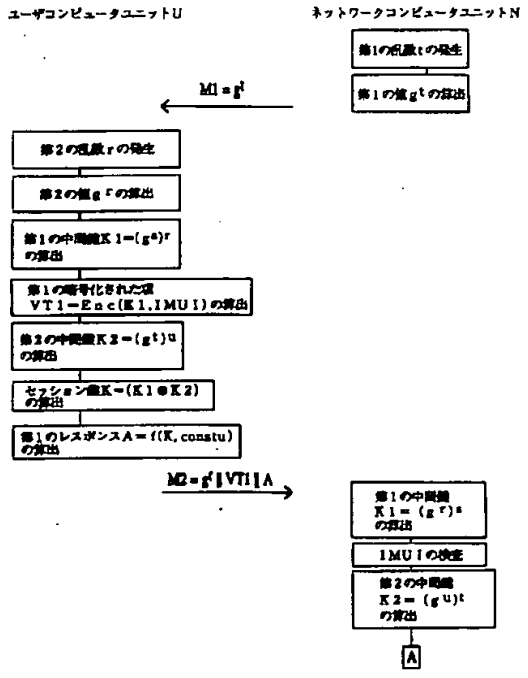
(71)出願人　シーメンス　アクチエンゲゼルシヤフト
ドイツ連邦共和国　Ｄ－80333　ミュンヘン　ヴィッテルスバッハープラッツ　2
(72)発明者　ギュンター　ホルン
ドイツ連邦共和国　Ｄ－81541　ミュンヘン　エードゥアルトーシュミットーシュトラーセ　16
(72)発明者　クラウス　ミュラー
ドイツ連邦共和国　Ｄ－81539　ミュンヘン　ラインターラー　シュトラーセ　15
(74)代理人　弁理士　矢野　敏雄　（外３名）

最終頁に続く

(54)【発明の名称】　ユーザコンピュータユニットUとネットワークコンピュータユニットNの間における暗号鍵のコンピュータ支援交換方法

(57)【要約】
本発明は暗号鍵の交換方法に関する。これによれば伝送されるメッセージの長さが低減され、この方法のセキュリティ特性は公知の方法よりも著しく拡大される。ネットワークコンピュータユニットとユーザコンピュータユニットにおいて、発せられた乱数に依存して第１の中間鍵と第２の中間鍵が生成される。これら第１の中間鍵と第２の中間鍵とをビットごとに排他ＯＲ結合することにより、セッション鍵が算出される。この鍵は絶対に平文では伝送されない。たとえば対称暗号化関数、ハッシュ関数または一方向性関数とすることのできる所定の関数を利用することにより、ネットワークコンピュータユニットとユーザコンピュータユニットが互いに認証され合う。

FIG 1a



【特許請求の範囲】

１．ユーザコンピュータユニット（Ｕ）とネットワークコンピュータユニット（Ｎ）の間における暗号鍵のコンピュータ支援交換方法において、

ネットワークコンピュータユニット（Ｎ）内で第１の乱数（ｔ）を生成し、

ネットワークコンピュータユニット（Ｎ）内で該第１の乱数（ｔ）から、１つの有限群における生成要素（ｇ）を用いることにより第１の値（g^t）を算出し、

ネットワークコンピュータユニット（Ｎ）において、少なくとも該第１の値（g^t）を含む第１のメッセージ（Ｍ１）を生成し、

該第１のメッセージ（Ｍ１）をネットワークコンピュータユニット（Ｎ）からユーザコンピュータユニット（Ｕ）へ伝送し、

ユーザコンピュータユニット（Ｕ）において第２の乱数（ｒ）を生成し、

ユーザコンピュータユニット（Ｕ）において該第２の乱数（ｒ）から、１つの有限群における生成要素（ｇ）を用いることで第２の値（g^r）を生成し、

ユーザコンピュータユニット（Ｕ）において、前記第２の乱数（ｒ）によりネットワーク公開鍵（ｇ

^{s}）を累乗することで第１の中間鍵（Ｋ１）を算出し、

ユーザコンピュータユニット（Ｕ）において、ユーザ秘密鍵（ｕ）により前記第１の値（g^t）を累乗することで第２の中間鍵（Ｋ１）を算出し、

ユーザコンピュータユニット（Ｕ）において、前記の第１の中間鍵（Ｋ１）と第２の中間鍵（Ｋ２）との結合によりセッション鍵（Ｋ）を算出し、

ユーザコンピュータユニット（Ｕ）において、少なくとも前記第２の値（g^r）を含む第２のメッセージ（Ｍ２）を生成し、

該第２のメッセージ（Ｍ２）をユーザコンピュータユニット（Ｕ）からネットワークコンピュータユニット（Ｎ）へ伝送し、

ネットワークコンピュータユニット（Ｎ）において、ネットワーク秘密鍵（ｓ）により前記第２の値（g^r）を累乗することで第１の中間鍵（Ｋ１）を算出し、

ネットワークコンピュータユニット（Ｎ）において、前記第１の乱数（ｔ）によりユーザ公開鍵（ｇu）を累乗することで第２の中間鍵（Ｋ２）を算出し、

ネットワークコンピュータユニット　（Ｎ）において、前記の第１の中間鍵（Ｋ１）と第２の中間鍵（Ｋ２）との結合によりセッション鍵（Ｋ）を算出することを特徴とする、

ユーザコンピュータユニット（Ｕ）とネットワークコンピュータユニット（Ｎ）の間における暗号鍵のコンピュータ支援交換方法。

２．ユーザコンピュータユニット（Ｕ）において、該ユーザコンピュータユニット（Ｕ）の身元識別情報（ＩＭＵＩ）を前記第１の中間鍵（Ｋ１）を用い暗号化関数（Ｅｎｃ）を利用して暗号化することで、第１の暗号化された項（ＶＴ１）を算出し、

前記第２のメッセージ（Ｍ２）に付加的に少なくとも該第１の暗号化された項（ＶＴ１）を含ませ、

ネットワークコンピュータユニット（Ｎ）において該第１の暗号化された項（ＶＴ１）を解読し、

ネットワークコンピュータユニット（Ｎ）においてユーザコンピュータユニット（Ｕ）の身元識別情報（ＩＭＵＩ）を検査する、

請求項１記載の方法。

３．ユーザコンピュータユニット（Ｕ）において、前記の第１の中間鍵（Ｋ１）と第２の中間鍵（Ｋ２）とのビットごとの排他ＯＲ結合によりセッション鍵（Ｋ）を算出し、

ネットワークコンピュータユニット（Ｎ）において、前記の第１の中間鍵（Ｋ１）と第２の中間鍵（Ｋ２）と’のビットごとの排他ＯＲ結合によりセッション鍵（Ｋ）を算出する、

請求項１または２記載の方法。

４．ユーザコンピュータユニット（Ｕ）において、ユーザ定数（ｃｏｎｓｔｕ）と前記セッション鍵（Ｋ）に対し関数（ｆ）を適用することで第１のレスポンス

（A）を生成し、

前記第2のメッセージ（M2）に付加的に少なくとも該第1のレスポンス（A）を含ませ、

ネットワークコンピュータユニット（N）において該第1のレスポンス（A）を検査する、

請求項1～3のいずれか1項記載の方法。

5．ネットワークコンピュータユニット（N）において、ネットワーク定数（constn）とセッション鍵（K）に対し関数（f）を適用することで第2のレスポンス（B）を生成し、

少なくとも該第2のレスポンスを含む第3のメッセージ（M3）をネットワークコンピュータユニット（N）からユーザコンピュータユニット（U）へ伝送し、

ユーザコンピュータユニット（U）において該第2のレスポンス（B）を検査する、

請求項1～4のいずれか1項記載の方法。

6．方法の開始にあたり認証メッセージをユーザコンピュータユニット（U）からネットワークコンピュータユニット（N）へ伝送し、該認証メッセージには認証コンピュータユニットにおける少なくとも1

つの識別情報が含まれ、該識別情報からユーザコンピュータユニット（U）により検証可能なネットワーク認証子（CertN）を送出させる、

請求項1～5のいずれか1項記載の方法。

7．前記第1のメッセージ（M1）には、ネットワークコンピュータユニット（N）におけるネットワークコンピュータ鍵（g^s）のネットワーク認証子（CertN）が付加的に含まれ、

ユーザコンピュータユニット（U）において該ネットワーク認証子（CertN）を検証し、

ユーザコンピュータユニット（U）において、該ユーザコンピュータユニット（U）におけるユーザ公開鍵（g^u）のユーザ認証子（CertU）を前記第

２の中間鍵（Ｋ１）を用い暗号化関数（Ｅｎｃ）を利用して暗号化することで第１の暗号化された項（ＶＴＩ）を生成し、

ネットワークコンピュータユニット（Ｎ）において該ユーザ認証子（Ｃｅｒｔｕ）を検証する、

請求項１～６のいずれか１項記載の方法。

８．前記関数（ｆ）は対称暗号化アルゴリズム、ハッシュアルゴリズムまたは一方向性関数であり、

ネットワークコンピュータユニット（Ｎ）における前記第１のレスポンス（Ａ）の検査にあたり、前記関数（ｆ）をユーザ定数（ｃｏｎｓｔｕ）とネットワークコンピュータユニット（Ｎ）内で算出され

たセッション鍵（Ｋ）とに対し適用し、その結果を前記第１のレスポンス（Ａ）との整合性について検査し、

ユーザコンピュータユニット（Ｕ）における前記第２のレスポンス（Ｂ）の検査にあたり、前記関数（ｆ）をネットワーク定数（ｃｏｎｓｔｎ）とユーザコンピュータユニット（Ｕ）内で算出されたセッション鍵（Ｋ）とに対し適用し、その結果を前記第２のレスポンス（Ｂ）との整合性について検査する、

請求項１～７のいずれか１項記載の方法。

９．前記関数（ｆ）は対称暗号化アルゴリズムであり、

ネットワークコンピュータユニット（Ｎ）における前記第１のレスポンス（Ａ）の検査にあたり、該第１のレスポンス（Ａ）をネットワークコンピュータユニット（Ｎ）において該ネットワークコンピュータユニット（Ｎ）内で算出されたセッション鍵（Ｋ）を用いて解読し、解読されたユーザ定数（ｃｏｎｓｔｕ′）を前記ユーザ定数（ｃｏｎｓｔｕ）と比較し、

ユーザコンピュータユニット（Ｕ）における前記第２のレスポンス（Ｂ）の検査にあたり、該第２のレスポンス（Ｂ）をユーザコンピュータユニット（Ｕ）において該ユーザコンピュータユニット（Ｕ

）内で算出されたセッション鍵（Ｋ）を用いて解読し、解読されたネットワーク

定数（ｃｏｎｓｔｎ′）を前記ネットワーク定数（ｃｏｎｓｔｎ）と比較する、

請求項１～８のいずれか１項記載の方法。

【発明の詳細な説明】

ユーザコンピュータユニットUとネットワークコンピュータユニットNの間における暗号鍵のコンピュータ支援交換方法

情報技術システムは様々な脅威に晒されている。たとえば伝送された情報が、権限のない第三者により盗み出されて変えられてしまうおそれがある。また、2つの通信パートナー間における別の脅威として挙げられるのが、一方の通信パートナーの偽の識別子を偽造することである。

これらの脅威やさらに別の脅威は種々のセキュリティメカニズムにより対処され、それによって情報技術システムがそれらの脅威から保護されるようにしている。安全性のために利用される1つのセキュリティメカニズムは伝送データの暗号化である。この場合、2つの通信パートナー間の通信交渉におけるデータを暗号化できるようにする目的で、オリジナルのデータを伝送する前に、暗号化を準備処理する第1のステップを実行する必要がある。このステップはたとえば次のようなものとすることができる。すなわち、両方の通信パートナーを1つの暗号化アルゴリズムに向けて合意させ、必要に応じて共通の秘密鍵の取り決めを行わせる。

暗号化によるセキュリティメカニズムが重要な意味をもつのは移動無線システムにおいてである。それというのも、このようなシステムにおいて伝送されるデータというのは、付加的に特別な手間をかけずとも第三者により盗み出せるからである。

したがって、情報技術システムのセキュリティが保証されるよう、公知のセキュリティメカニズムの選択を行って、それらのセキュリティメカニズムを適切に組み合わせ、さらに通信プロトコルを指定しなければならない。

暗号鍵のコンピュータ支援交換を行うための種々の非対称方式が公知である。移動無線システムに適した非対称方式は、A. Aziz, W, Diffie 著の "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1994, p. 25-31, および M. Beller 著の "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and

Authentication for Personal Communications, P&A JEM 1993, p. 1-11 である。

A. Aziz, W, Diffie 著の "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1994, p. 25-31 に記載されている方法は、明らかにローカルネットワークに係わるものであり、暗号鍵交換にあたり各通信パートナーのコンピュータユニットに対し、著しく高い所要計算能力を課すものである。しかもこの方法の場合、本発明による方法よりも大きな伝送キャパシティが必要とされる。それというのも、メッセージの長さが本発明による方法の場合よりも長いからである。

また、 M. Beller 著の "Proposed Authentication and Key Agreement Protocol for PCS", Joint Experts Meeting on Privacy and Authentication for Personal Communications, P&A JEM 1993, p. 1-11 は、いくつかの基本的なセキュリティメカニズムを統合していない。この場合、ユーザによる明示的なネットワークの認証が実現されない。しかもこの場合、ユーザからネットワークへ伝送される鍵は、ネットワークによりユーザに対し受領確認されない。さらに、ネットワークのための鍵の更新（アップデート）も行われない。この方法のさらに別の欠点は、ユーザによる鍵の暗黙的な認証がラビン方式に限られていることである。これにより、この方法はフレキシブルな適用の点で制限されてしまう。しかも、伝送データが疑う余地のないものであることを保証するセキュリティメカニズムも設けられていない。このことは殊に、移動無線システムに関する疑う余地のない料金決済を作成する場合にも重大な欠点となる。また、この方法は利用される署名機能として National Institue of Standard in Technology Signature Standard (NIST DSS) に限定されていることでも、一般的な用途の点でこの方法は制限されている。

したがって本発明の課題は、これまで述べてきた欠点を回避するようにした暗号鍵のコンピュータ支援交換方法を提供することにある。

この課題は、請求項1に記載の方法により解決される。

本発明による方法により達せられる利点は殊に、公知の方法に比べて本発明に

よる方法の安全性が著しく高い点と、伝送されるメッセージの長さが著しく低減される点にある。本発明による方法によれば、以下のセキュリティメカニズムが実現される：

－ユーザ側とネットワーク側の双方で行われる明示的な認証、すなわち主張する身元識別情報の双方での検証

－双方で行われる暗黙的な認証を伴うユーザ側とネットワーク側との間の鍵の取り決め、すなわち本発明による方法によれば、手順完了後、１つの共通のセッション秘密鍵が利用可能となり、そのうち各々の当事者が知っているのは、認証された相手だけがやはりセッション秘密鍵を所有できるということである。

－ユーザおよびネットワークに対するセッション鍵更新（アップデート）の保証

－ユーザ側とネットワーク側の双方で行われるセッション鍵の承認、すなわち取り決められたセッション

秘密鍵を相手が本当に所有していることの承認

－ユーザの匿名性、すなわち第三者に対するユーザ身元情報の機密性

－ユーザによりユーザからネットワークへ送信されたデータの明白性

－ネットワークからユーザへのネットワーク公開鍵に対する認証の送信

－認証権限からネットワークへのユーザ公開鍵に対する承認の送信

さらに本発明による方法により得られる格別な利点として挙げられるのは、対称暗号化アルゴリズムと比べ著しく計算量の多いモジュラべき乗（modular exponentiation）を各側で２回だけ実行すればよいことであり、このことにより著しく高いプロトコル処理レートが可能となる。

請求項３による本発明による方法の実施形態によれば付加的にさらに別のセキュリティメカニズムが実現され、ユーザ側とネットワーク側との間の公開鍵に対する認証の交換が実現される。

しかも本発明による方法によれば、きわめて容易に種々の要求に整合させることができる。それというのも本発明は特定の暗号化アルゴリズムに限定されるものではないからである。

従属請求’項には、以下で詳述する本発明の有利な実施例が示されている。

図１ａ，ｂは、請求項１記載の本発明による方法を表したフローチャートである。

図２ａ，ｂは、請求項３記載の本発明による方法を表した図である。

次に、図１ａ，ｂおよび図２ａ，ｂを参照しながら本発明について説明する。

図１ａ，ｂには、請求項１記載の本発明による方法のシーケンスが描かれている。この方法において前提とするのは、ユーザコンピュータユニットＵにおいて信頼できるネットワーク公開鍵g^sを利用できることである。しかもこの場合、ネットワークコンピュータユニットＮにおいて信頼できるユーザ公開鍵g^uを利用できるものとする。

図１ａ，ｂに示されている本発明による方法は、ネットワークコンピュータユニットＮにおける第１の乱数ｔの生成から始まる。そしてこの第１の乱数ｔから、ネットワークコンピュータユニットＮにおいて有限群の生成要素ｇにより第１の値g^tが形成される。

非対称の方法は実質的に複雑性理論における２つの問題に基づくものであり、合成数を効率的に因数分解する問題と離散的対数問題（ＤＬＰ）である。ＤＬＰというのは、適切な計算構造においてたしかに指数計算は効率的に実行できるが、逆の演算操作つまり対数計算のためには効率的なアルゴリズムは知られていない、ということである。この種の計算構造は、上述の

有限群のもとで解されなければならない。これはたとえば有限体の乗法的群（たとえばモジュロｐの乗算ただしｐは大きい素数）あるいはいわゆる”楕円曲線”である。楕円曲線が注目されるのは殊に、これにより同じセキュリティレベルでも著しく短いセキュリティパラメータが可能となるからである。そしてこれは公開鍵の長さ、証明情報の長さ、セッションキーの取り決めにあたり交換すべきメッセージの長さ、ならびにディジタル署名の長さが該当し、これらについてはあとで説明する。その理由は、楕円曲線に関して既知である対数計算手法は有限体に対するものよりもかなり効率が悪いからである。この関連で大きい素数が意味するのは、是認できる時間内では実行できないほど対数計算が複雑となるよう、素数の大きさを選定する必要のあることである。ここにおいて、”是認できる”

とは、情報技術システムのためのセキュリティ方針に応じて数年～数１０年さらにはそれ以上の期間を意味する。

第１の値ｇ^{t}の算出後、少なくともこの第１の値ｇ^{t}を有する第１のメッセージＭ１が形成される。第１のメッセージＭ１はネットワークコンピュータユニットＮにより符号化され、ユーザコンピュータユニットＵへ伝送される。そしてユーザコンピュータユニットＵにおいで、この第１のメッセージＭが復号される。

さらにユーザコンピュータユニットＵにおいて、第

２の乱数ｒが形成される。この第２の乱数ｒから、選択された上述の計算構造に応じて生成要素ｇにより第２の値ｇ^{r}が算出される。

ユーザコンピュータユニットにおいて利用可能なネットワーク公開鍵は第２の乱数ｒにより累乗され、これにより第１の中間鍵Ｋ１が生成される。

第１の中間鍵Ｋ１を用いることで、暗号化アルゴリズムＥｎｃを使用してユーザコンピュータユニットＵの身元識別情報ＩＭＵＩが暗号化される。暗号化された身元識別情報ＩＭＵＩにより暗号化された第１の項ＶＴ１が形成される。

さらにユーザコンピュータユニットＵにおいて、第１の値ｇ^{t}をユーザ秘密鍵ｕで累乗することにより第２の中間鍵Ｋ２が算出される。

第１の中間鍵Ｋ１と第２の中間鍵Ｋ２に対しビットごとに排他ＯＲ関数を適用することにより、セッション鍵Ｋが算出される。関数ｆを利用したセッション鍵Ｋを用いて、ユーザコンピュータユニットＵにもネットワークコンピュータユニットＮにも既知であるユーザ定数ｃｏｎｓｔｕの暗号化により、第１のレスポンスＡが形成される。

この関数ｆはたとえば対称暗号関数とすることもできるし、あるいはハッシュ関数または一方向性関数とすることもできる。この関連で一方向性関数とは、所定の関数値に対し合致する入力値を計算することが不

可能な関数のことである。また、ハッシュ関数とは圧縮形の一方向性関数のことであり、ハッシュ関数においては任意の長さの入力キャラクタ列が固定長の出力キャラクタ列にマッピングされる。さらにこの関連で、一方向性関数ないしハッ

シュ関数について不調和がないようにしなければならず、つまり同じ出力キャラクタ列を生じさせる異なる２つの入力キャラクタ列があってはならない。既知のハッシュ関数はたとえばＭＤ２アルゴリズムまたはＭＤ５アルゴリズムである。

次に、ユーザコンピュータユニットＵにおいて第２のメッセージＭ２が生成され、その際、メッセージＭ２には少なくとも第２の値g^rと、暗号化された第１の項ＶＴ１と、第１のレスポンスＡが含まれている。第２のメッセージＭ２はユーザコンピュータユニットＵにおいて符号化され、ネットワークコンピュータユニットＮへ伝送される。

第２のメッセージＭ２において伝送される第２の値g^rによりネットワークコンピュータユニットＮは、第１の中間鍵Ｋ１を伝送する必要なく第１の中間鍵Ｋ１自体を生成することが可能となる。このことが達成される理由は、ユーザコンピュータユニットＵとネットワークコンピュータユニットＮだけが第１の中間鍵Ｋ１を所有しているからである。

第１のレスポンスＡはセッション鍵の検証に用いられ、これは後で述べるように、セッション鍵Ｋを伝送

する必要なくネットワークコンピュータユニットＮによっても生成可能である。

ネットワークコンピュータユニットＮにおいて第２のメッセージＭ２の受信後、この第２のメッセージＭ２が復号される。続いてネットワークコンピュータユニットＮにおいて第１の中間鍵Ｋ１が計算され、これは第２の値g^rをネットワーク秘密鍵ｓで累乗することにより行われる。これによりネットワークコンピュータユニットＮは、伝送された第１の暗号化された項ＶＴ１を事前に計算された第１の中間鍵Ｋ１により解読することができる。

第１の暗号化された項ＶＴ１の解読が実行され、これによりユーザコンピュータユニットＵは第１のメッセージＭ２の送信者として認証される。信頼性をもってネットワークコンピュータユニットＮにおいて利用可能なユーザ公開鍵g^uの累乗から、ネットワークコンピュータユニットＮにおいて第１の乱数ｔを用いることで第２の中間鍵Ｋ２が生成される。

セッション鍵ＫはネットワークコンピュータユニットＮにおいてもユーザコン

ピュータユニットUにおいても、第１の中間鍵Ｋ１と第２の中間鍵Ｋ２とのビットごとの排他ＯＲ結合により算出される。

セッション鍵Ｋを用い関数ｆを利用することで第１のレスポンスＡが検査される。この検査は、関数ｆがどのような形式のものであるかに応じて、様々なやり方で行うことができる。

ユーザコンピュータユニットUにおける明示的な認証は第１のレスポンスＡにより達成される。それというのも、ネットワークコンピュータユニットN以外にはユーザコンピュータユニットUだけしかセッション鍵Ｋを知らないからである。

関数ｆが対称暗号関数により実現される場合、第１のレスポンスＡの検査は２とおりの形式で実施することができる。

ネットワークコンピュータユニットNにとって既知であるユーザ定数ｃｏｎｓｔｕは、セッション鍵Ｋを用い関数ｆを利用することでネットワークコンピュータユニットNにより暗号化することができ、その結果を第１のレスポンスＡとそのまま比較することができる。その結果が第１のレスポンスＡと一致しているならば、鍵Ｋの正当性が保証されることになる。

しかし、第１のレスポンスＡをネットワークコンピュータユニットNにおいて算出されたセッション鍵を用いて解読することも可能であり、これにより得られた解読されたユーザ定数ｃｏｎｓｔｕ′を既知のユーザ定数ｃｏｎｓｔｕと比較することができる。ユーザ定数ｃｏｎｓｔｕが解読されたユーザ定数ｃｏｎｓｔｕ′と一致しているならば、やはりセッション鍵Ｋの正当性が保証されることになる。

関数ｆがハッシュ関数により実現されている場合、

第１のレスポンスＡの解読は当然ながら不可能である。したがってこの事例の場合には、関数ｆを利用することでユーザ定数ｃｏｎｓｔｕとセッション鍵Ｋにより第１のレスポンスＡと比較される結果が送出されるよう、検査を行うことだけが可能である。

次にネットワークコンピュータユニットＮにおいて、関数ｆを利用することでネットワーク定数ｃｏｎｓｔｎが検査されるセッション鍵Ｋにより暗号化され、第２のレスポンスＢが生成される。

さらにネットワークコンピュータユニットＮにおいて、少なくとも第２のレスポンスＢを含む第３のメッセージＭ３が生成される。この第３のメッセージＭ３はネットワークコンピュータユニットＮにより符号化され、ユーザコンピュータユニットＵへ伝送される。

そしてユーザコンピュータユニットＵにおいて第３のメッセージＭ３が復号され、これに続いて、ネットワークコンピュータユニットＮにおける第１のレスポンスＡについて先に述べたのと同じようにして、第２のレスポンスが検査される。

ユーザコンピュータユニットＵにおいてネットワーク公開鍵g^sが、ネットワークコンピュータユニットＮにおいてユーザ公開鍵g^uが既知でなく、ないしは信頼性を伴って存在していない場合には、請求項３記載の本発明による方法の実施形態が適用される。図２ａ、ｂには本発明のこの実施形態が示されている。

ネットワーク公開鍵g^sとユーザ公開鍵g^uを交換するために、ユーザ認証子ＣｅｒｔＵとネットワーク認証子ＣｅｒｔＮが設けられている場合に有利であるのは、信頼性のある複数の認証権限が存在しているときにユーザコンピュータユニットＵがネットワークコンピュータユニットＮへ、どの認証権限によりユーザコンピュータユニットＵがネットワーク認証子ＣｅｒｔＮを検証できるのかを通報することである。

このことはたとえば、本発明による方法の開始にあたり認証メッセージをユーザコンピュータユニットＵからネットワークコンピュータユニットＮへ伝送することにより行える。この関連で認証メッセージは認証コンピュータユニットにおける少なくとも１つの識別情報を有しており、それからネットワークコンピュータユニットＮはネットワーク認証子ＣｅｒｔＮを得ることができ、これをユーザコンピュータユニットＵにより検証することができる。

ネットワークコンピュータユニットＮが認証コンピュータユニットＣＡからネ

ットワーク認証子ＣｅｒｔＮを得た後、そのネットワーク認証子ＣｅｒｔＮはユーザコンピュータユニットＵへ伝送される。

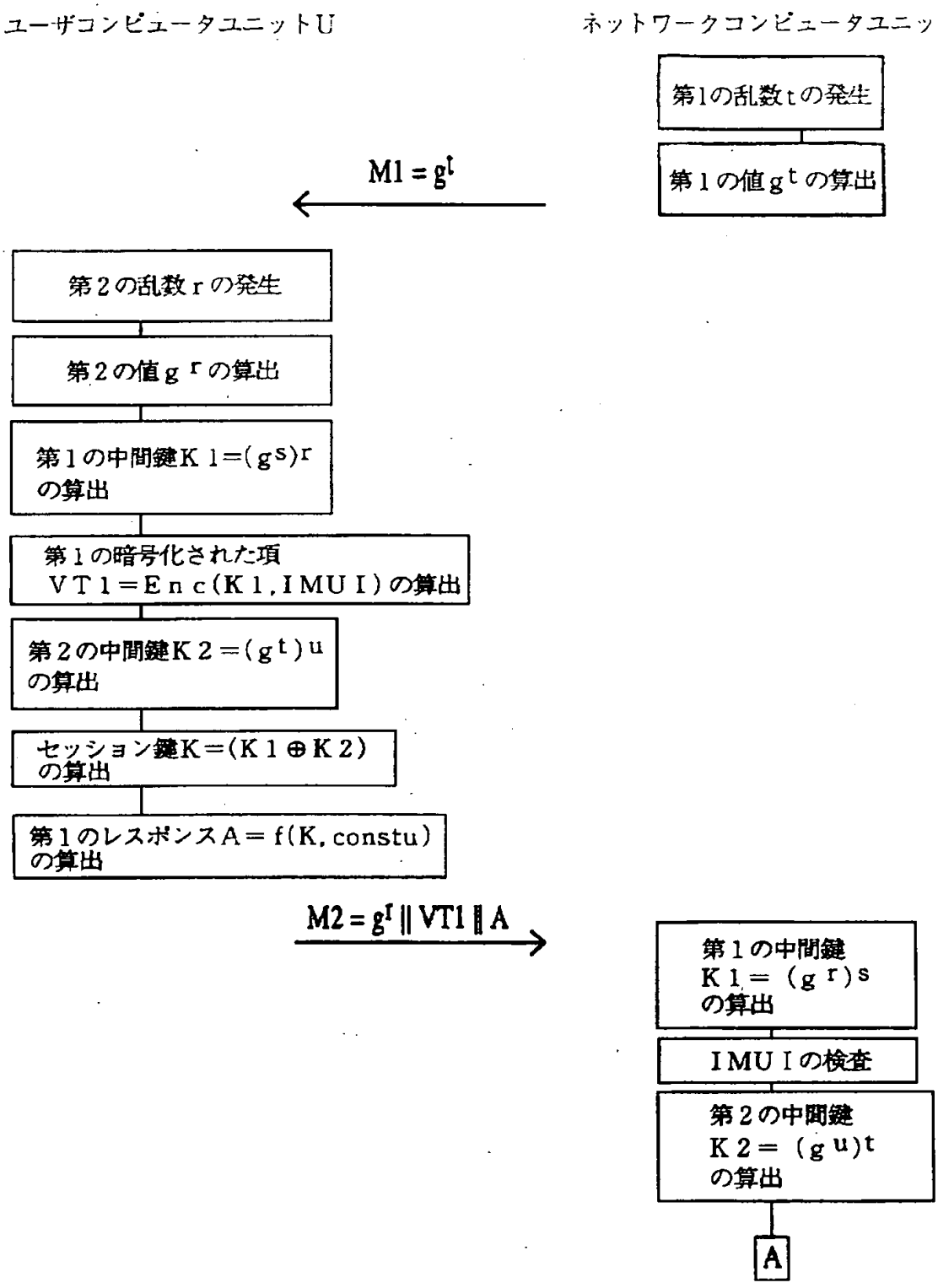
このことは、第１のメッセージＭ１に付加的にネットワーク認証子ＣｅｒｔＮが添付されることにより行われる。この事例の場合、ユーザコンピュータユニットＵにおいて第１のメッセージＭ１の復号後、ネット

ワーク認証子ＣｅｒｔＮの検証が行われ、このことでユーザコンピュータユニットＵは信頼性のあるネットワーク公開鍵g^sを得ることになる。

他方、ユーザコンピュータユニットＵではユーザ認証子ＣｅｒｔＵが求められ、これはユーザコンピュータユニットＵの身元識別情報ＩＭＵＩの代わりに第１の中間鍵Ｋ１を用い暗号化関数Ｅｎｃを利用して暗号化され、第１の暗号化された項ＶＴ１が生成される。このようにして、ユーザコンピュータユニットＵの正体が第２のメッセージＭ２の伝送時に権限のない第三者のところで明らかにされてしまうことなく、ユーザ認証子ＣｅｒｔＵの伝送が可能となる。ネットワークコンピュータユニットＮにおいて第１の項ＶＴ１が解読された後、このようにして得られたユーザ認証子ＣｅｒｔＵがネットワークコンピュータユニットＮにより検証される。このようにして、ネットワーク識別子ＣｅｒｔＮとユーザ認証子ＣｅｒｔＵの信頼性のある交換が実現される。

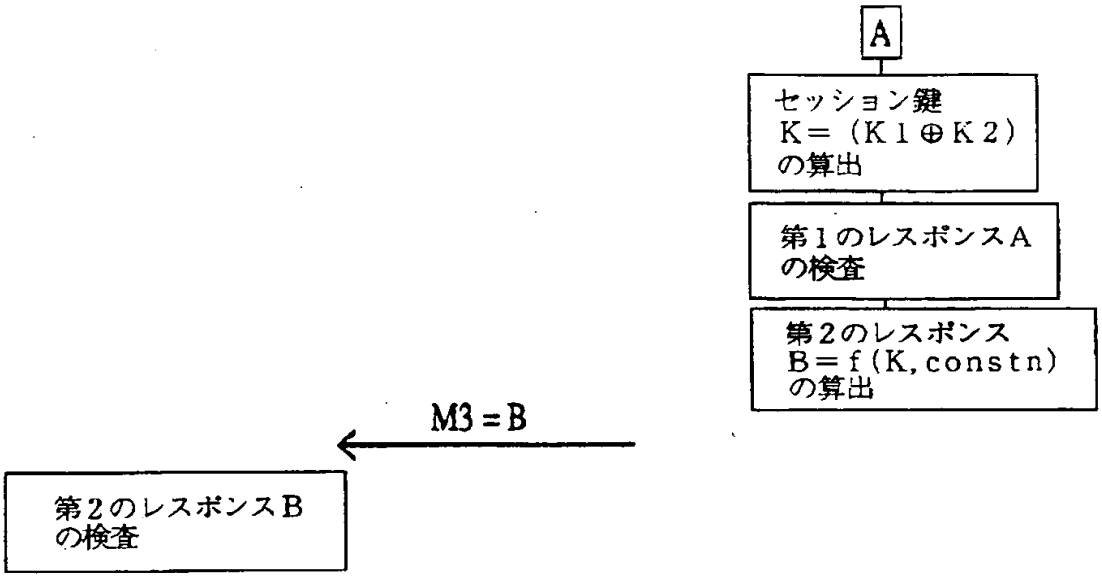
【図１ａ】

FIG 1a


ユーザコンピュータユニットU
ネットワークコンピュータユニットN
第1の乱数tの発生
第１の値ｇ t の算出
M1 = g t
第２の乱数ｒの発生
第２の値ｇ r の算出
第１の中間鍵Ｋ１＝(ｇS)r の算出
第１の暗号化された項 ＶＴ１＝Ｅｎｃ(Ｋ１,ＩＭＵＩ)の算出
第２の中間鍵Ｋ２＝(ｇt)u の算出
セッション鍵Ｋ＝(Ｋ１⊕Ｋ２) の算出
第１のレスポンスＡ＝ｆ(Ｋ, constu) の算出
M2 = g r ‖ VT1 ‖ A
第１の中間鍵 Ｋ１＝（ｇ r)s の算出
ＩＭＵＩの検査
第２の中間鍵 Ｋ２＝（ｇu)t の算出
A

【図１】

FIG 1b


A
セッション鍵
K＝（K１⊕K２）
の算出
第１のレスポンスA
の検査
第２のレスポンス
B＝f（K,constn）
の算出
M3＝B
第２のレスポンスB
の検査

【図２】

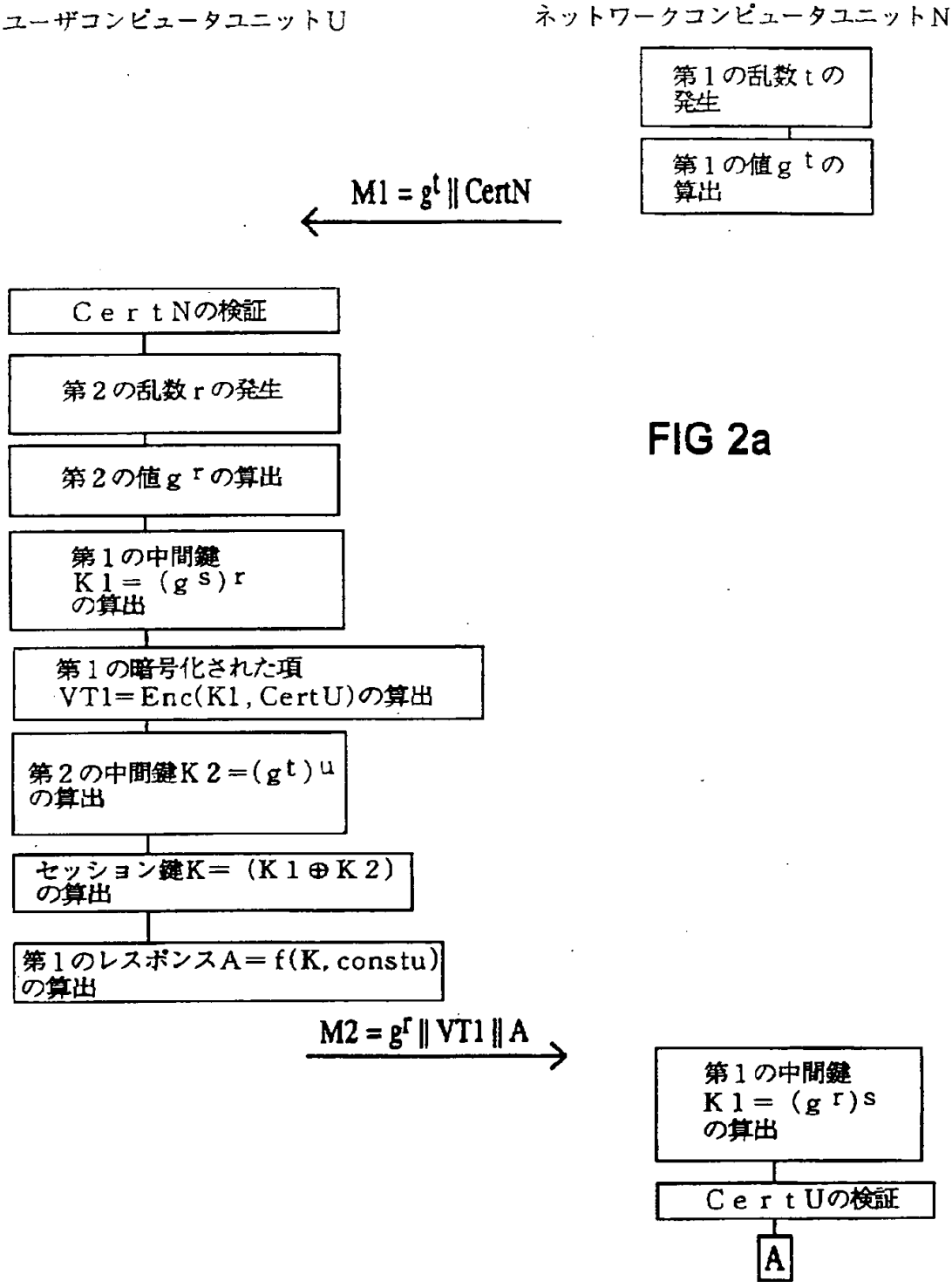
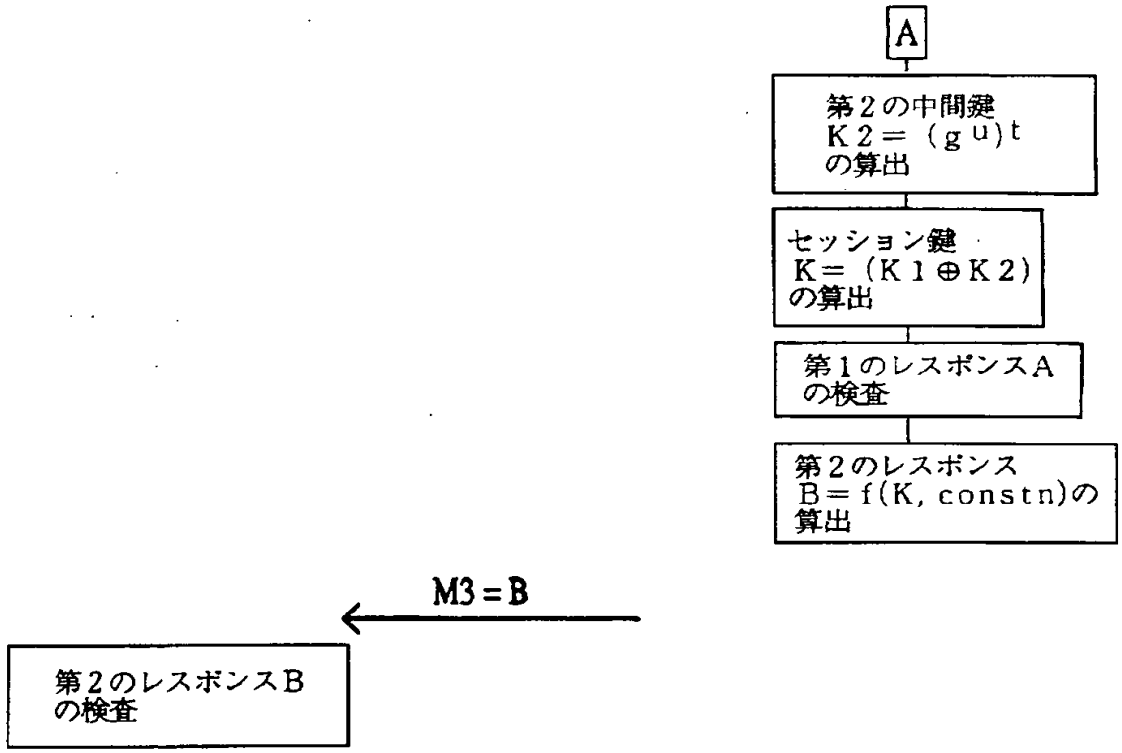

ユーザコンピュータユニットU
ネットワークコンピュータユニットN
第１の乱数ｔの発生
第１の値ｇｔの算出
M1 = g^t || CertN
ＣｅｒｔＮの検証
第２の乱数ｒの発生
第２の値ｇｒの算出
第１の中間鍵 Ｋ１＝（ｇｓ）ｒ の算出
第１の暗号化された項 VT1=Enc(K1, CertU)の算出
第２の中間鍵Ｋ２＝(ｇｔ)ｕ の算出
セッション鍵Ｋ＝（Ｋ１⊕Ｋ２）の算出
第１のレスポンスA＝f(K, constu)の算出
M2 = g^r || VT1 || A
第１の中間鍵 Ｋ１＝（ｇｒ）ｓ の算出
ＣｅｒｔＵの検証
A

FIG 2a

【図２】

FIG 2b


A
第２の中間鍵
Ｋ２＝（ｇｕ）ｔ
の算出
セッション鍵
Ｋ＝（Ｋ１⊕Ｋ２）
の算出
第１のレスポンスＡ
の検査
第２のレスポンス
Ｂ＝ｆ(Ｋ, ｃｏｎｓｔｎ)の
算出
M3＝B
第２のレスポンスＢ
の検査

【手続補正書】特許法第１８４条の８第１項

【提出日】１９９７年１月２１日

【補正内容】

３．ユーザコンピュータユニット（Ｕ）において、前記の第１の中間鍵（Ｋ１）と第２の中間鍵（Ｋ２）とのビットごとの排他ＯＲ結合によりセッション鍵（Ｋ）を算出し、

ネットワークコンピュータユニット（Ｎ）において、前記の第１の中間鍵（Ｋ１）と第２の中間鍵（Ｋ２）とをビットごとに排他ＯＲ結合することによりセッション鍵（Ｋ）を算出する、

請求項１または２記載の方法。

４．ユーザコンピュータユニット（Ｕ）において第１のレスポンス（Ａ）を、ユーザ定数（ｃｏｎｓｔｕ）と前記セッション鍵（Ｋ）に対し関数（ｆ）を適用することにより生成し、

前記第２のメッセージ（Ｍ２）は付加的に少なくとも該第１のレスポンス（Ａ）を有し、

ネットワークコンピュータユニット（Ｎ）において該第１のレスポンス（Ａ）を検査する、

請求項１～３のいずれか１項記載の方法。

５．ネットワークコンピュータユニット（Ｎ）において第２のレスポンス（Ｂ）を、ネットワーク定数（ｃｏｎｓｔｎ）とセッション鍵（Ｋ）に対し関数（ｆ）を適用することにより生成し、

少なくとも該第２のレスポンスを含む第３のメッセージ（Ｍ３）をネットワークコンピュータユニット（Ｎ）からユーザコンピュータユニット（Ｕ）へ

伝送し、

ユーザコンピュータユニット（Ｕ）において該第２のレスポンス（Ｂ）を検査する、

請求項１～４のいずれか１項記載の方法。

６．方法の開始にあたり認証メッセージをユーザコンピュータユニット（Ｕ）か

らネットワークコンピュータユニット（Ｎ）へ伝送し、該認証メッセージには認証コンピュータユニットにおける少なくとも１つの識別情報が含まれ、該識別情報からユーザコンピュータユニット　（Ｕ）により検証可能なネットワーク認証子（ＣｅｒｔＮ）を送出させる、

請求項１～５のいずれか１項記載の方法。

７．前記第１のメッセージ（Ｍ１）には、ネットワークコンピュータユニット（Ｎ）におけるネットワークコンピュータ鍵（g^s）のネットワーク認証子（ＣｅｒｔＮ）が付加的に含まれ、

ユーザコンピュータユニット（Ｕ）において該ネットワーク認証子（ＣｅｒｔＮ）を検証し、

ユーザコンピュータユニット（Ｕ）において、該ユーザコンピュータユニット（Ｕ）におけるユーザ公開鍵（g^u）のユーザ認証子（ＣｅｒｔＵ）を前記第２の中間鍵（Ｋ１）を用い暗号化関数（Ｅｎｃ）を利用して暗号化することで第１の暗号化された項（ＶＴ１）を生成し、

ネットワークコンピュータユニット（Ｎ）におい

て該ユーザ認証子（ＣｅｒｔＵ）を検証する、

請求項２または請求項２に依存するかぎり請求項３～６のいずれか１項記載の方法。

８．前記関数（ｆ）は対称暗号化アルゴリズム、ハッシュアルゴリズムまたは一方向性関数であり、

ネットワークコンピュータユニット（Ｎ）における前記第１のレスポンス（Ａ）の検査にあたり、前記関数（ｆ）をユーザ定数（ｃｏｎｓｔｕ）とネットワークコンピュータユニット（Ｎ）内で算出されたセッション鍵（Ｋ）とに対し適用し、その結果を前記第１のレスポンス（Ａ）との整合性について検査し、

ユーザコンピュータユニット（Ｕ）における前記第２のレスポンス（Ｂ）の検査にあたり、前記関数（ｆ）をネットワーク定数（ｃｏｎｓｔｎ）とユーザコンピュータユニット（Ｕ）内で算出されたセッション鍵（Ｋ）とに対し適用し、その結果を前記第２のレスポンス（Ｂ）との整合性について検査する、

請求項１～７のいずれか１項記載の方法。

９．前記関数（ｆ）は対称暗号化アルゴリズムであり、

ネットワークコンピュータユニット（Ｎ）における前記第１のレスポンス（Ａ）の検査にあたり、該第１のレスポンス（Ａ）をネットワークコンピュータユニット（Ｎ）において該ネットワークコンピュータユニット（Ｎ）内で算出されたセッション鍵（Ｋ）を用いて解読し、解読されたユーザ定数（ｃｏｎｓｔｕ′）を前記ユーザ定数（ｃｏｎｓｔｕ）と比較し、

ユーザコンピュータユニット（Ｕ）における前記第２のレスポンス（Ｂ）の検査にあたり、該第２のレスポンス（Ｂ）をユーザコンピュータユニット（Ｕ）において該ユーザコンピュータユニット（Ｕ）内で算出されたセッション鍵（Ｋ）を用いて解読し、解読されたネットワーク定数（ｃｏｎｓｔｎ′）を前記ネットワーク定数（ｃｏｎｓｔｎ）と比較する、

請求項４または５記載の方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/DE 96/00591

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 393 806 (TRW) 24 October 1990 see column 5, line 25 - column 6, line 5 see column 6, line 35 - line 41 see column 10, line 45 - column 11, line 8 ---	1,3
A	IEE PROCEEDINGS-COMPUTERS AND DIGITAL TECHNIQUES, MAY 1994, UK, vol. 141, no. 3, ISSN 1350-2387, pages 193-195, XP000454518 HARN L: "Public-key cryptosystem design based on factoring and discrete logarithms" see page 194, left-hand column, line 27 - line 42 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 July 1996	26. 08. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna tal Application No
PCT/DE 96/00591

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PROCEEDINGS. THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS 28TH ANNUAL 1994 INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY (CAT. NO.CH3437-1/94), PROCEEDINGS OF IEEE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY, ALBUQUER, ISBN 0-7803-1479-4, 1994, NEW YORK, NY, USA, IEEE, USA, pages 76-79, XP000492106 WITZKE E L ET AL: "Key management for large scale end-to-end encryption" see page 77, right-hand column, last paragraph - page 78, left-hand column, line 8 see page 79, left-hand column, line 37 - line 43 -----	1

INTERNATIONAL SEARCH REPORT

.formation on patent family members

Interr al Application No
PCT/DE 96/00591

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-393806	24-10-90	US-A-	4956863	11-09-90
		JP-A-	2288746	28-11-90

フロントページの続き

(72)発明者　フォルカー　ケスラー
ドイツ連邦共和国　Ｄ－85256　フィーア
キルヒェン　プファラーーシュミッターー
シュトラーセ　1